MORDELL-WEIL RANKS OF FAMILIES OF ELLIPTIC CURVES ASSOCIATED TO PYTHAGOREAN TRIPLES

BARTOSZ NASKRĘCKI

Abstract. We study the family of elliptic curves $y^2 = x(x-a^2)(x-b^2)$ parametrized by Pythagorean triples (a, b, c). We prove that for a generic triple the lower bound of the rank of the Mordell-Weil group over $\mathbb{Q}$ is 1, and for some explicitly given infinite family the rank is 2. To each family we attach an elliptic surface fibered over the projective line. We show that the lower bounds for the rank are optimal, in the sense that for each generic fiber of such an elliptic surface its corresponding Mordell-Weil group over the function field $\mathbb{Q}(t)$ has rank 1 or 2, respectively. In order to prove this, we compute the characteristic polynomials of the Frobenius automorphisms acting on the second ℓ-adic cohomology groups attached to elliptic surfaces of Kodaira dimensions 0 and 1.

1. Introduction

Consider a triple of integers a, b and c that satisfy the Pythagorean equation

$$a^2 + b^2 = c^2.$$

We intend to study a family of elliptic curves $E_{(a,b,c)}$

$$y^2 = x(x-a^2)(x-b^2) \tag{1.1}$$

parametrized by such triples. The family (1.1) is similar to another family of curves

$$y^2 = x(x-a^2)(x+b^2) \tag{1.2}$$

with $a^2 + b^2 = c^2$ which is a special case the well-known Frey family. For low conductors there are many curves of high Mordell-Weil rank (up to rank 6) in the family (1.1). This is, however, usually not the case for the family (1.2), since generically it is of rank 0.

The family (1.1) is equivalent to the family of curves in the Legendre form

$$y^2 = x(x-1)(x-\lambda)$$

with the parameter λ limited to rational numbers of the form

$$\lambda = \left(\frac{2s}{s^2-1}\right)^2,$$

for s rational, not equal to 0 or 1. The Mordell-Weil rank of the family (1.1) was considered for the first time in the paper [6], where it was proven that the group $E_{(a,b,c)}(\mathbb{Q})$ of rational points contains a point (c^2, abc) of infinite order.

In order to state our results, we need some extra notation. Consider the set

$$\mathcal{T} = \{(a,b,c) \in \mathbb{Z}^3 : a^2 + b^2 = c^2, \quad GCD(a,b,c) = 1, \quad ab(a^2-b^2) \neq 0\}$$

of triples of pairwise coprime integers that satisfy the Pythagorean equation and define a smooth curve in the family (1.1). For any triple $(a, b, c) \in \mathcal{T}$, the rank of the Mordell-Weil group of rational points on $y^2 = x(x-a^2)(x-b^2)$ is at least one by [6, Lemma 6.8]. We define an infinite

subset $\mathcal{S}$ of $\mathcal{T}$. A triple (a, b, c) belongs to $\mathcal{S}$ if and only if its coordinates can be written in the form

$$\begin{aligned} a &= P^2 - Q^2, \\ b &= 2PQ, \\ c &= P^2 + Q^2, \end{aligned}$$

where the fraction $\frac{P}{Q} = \frac{2pq}{p^2+5q^2}$ is in its lowest terms and $p, q \in \mathbb{Z}$ are coprime integers.

Our first main result is the following statement.

Theorem 1.1. *For all but finitely many $(a, b, c) \in \mathcal{S}$ the curve*

$$y^2 = x(x - a^2)(x - b^2)$$

has the Mordell-Weil group of rank at least two. There are two linearly independent points

$$Q_1 = \left(\frac{1}{2}(a+b-c)^2, \frac{1}{2}(a+b)(a+b-c)^2\right),$$

$$Q_2 = \left(\frac{1}{2}a(a-c), \frac{1}{2}ab\frac{1}{k^2}\left(p^4 - 25q^4\right)\right),$$

where $k = GCD(2pq, p^2 + 5q^2)$ and p and q are as above.

Concerning the generic rank of family (1.1) we have the following result.

Theorem 1.2. *The group of $\mathbb{Q}(t)$-rational points on the curve*

$$y^2 = x(x-1)(x - \left(\frac{2t}{t^2-1}\right)^2) \tag{1.3}$$

is of rank one.

We prove Theorem 1.2 as an application of the Shioda-Tate formula. In fact, a stronger result holds. The rank of the group of $\overline{\mathbb{Q}}(t)$-rational points of the curve from Theorem 1.1 is equal to 2 but only a subgroup of rank one is defined over $\mathbb{Q}(t)$. Similar investigation of the generic rank of the family (1.2) shows that the rank of the Mordell-Weil group of the corresponding model over $\overline{\mathbb{Q}}(t)$ is equal to 0.

The result in Theorem 1.1 displays the generic rank but the corresponding geometric result is more involved.

Theorem 1.3. *Let*

$$E: \quad y^2 = x\left(x - \left(\left(\frac{2t}{t^2+5}\right)^2 - 1\right)^2\right)\left(x - 4\left(\frac{2t}{t^2+5}\right)^2\right),$$

be the elliptic curve over $\overline{\mathbb{Q}}(t)$ which is obtained from the curve (1.3) by a suitable change of parameter t and a linear change of coordinates (cf. formula (6.1)). The geometric Mordell-Weil group $E(\overline{\mathbb{Q}}(t))$ is isomorphic to $\mathbb{Z}^3 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. We put $u = \frac{2t}{t^2+5}$. The free part of the group $E(\overline{\mathbb{Q}}(t))$ is generated by the points

$$\begin{aligned} P_1 &= (2(1+\sqrt{2})(-1+u)^2u, 2\sqrt{-1}(1+\sqrt{2})(-1+(\sqrt{2}-u)^2)(-1+u)^2u), \\ P_2 &= (2(u-1)^2, 2(-1+u)^2(-1+2u+u^2)), \\ P_3 &= \left(1-u^2, \frac{(-5+t^2)\,u\,(-1+u^2)}{5+t^2}\right). \end{aligned}$$

The torsion subgroup of $E(\overline{\mathbb{Q}}(t))$ is generated by points

$$T_1 = (-4u^2, 0)$$
$$T_2 = (2(-u+u^3), 2\sqrt{-1}(u^2-1)u(-1-2u+u^2)).$$

Moreover the group of $\mathbb{Q}(t)$-rational points on E is generated by the points P_2, P_3 and T_1 and $2T_2$.

The proof of Theorem 1.3 requires more involved methods. Note that the geometric approach of Shioda, cf. [15] implies only that the upper bound of the rank equals 6. We base the proof of Theorem 1.3 on the approach of van Luijk in [20] and Kloosterman in [8].

To the best of our knowledge, the method of van Luijk and Kloosterman was used in the past exclusively for rational or K3 surfaces, cf. [13], [19], [18] and [5]. If an elliptic surface is of high geometric genus, then the method described below becomes very ineffective and it is computationally difficult to determine the zeta function of the surface. In our case, we perform calculations on elliptic sufaces which are rational or K3. In particular, we attach to the elliptic curve E over $\overline{\mathbb{Q}}(t)$ an elliptic surface over $\mathbb{P}^1$, cf. [2]. We find its integral model S as a scheme over A, where A is a discrete valuation ring of a number field with a residue field isomorphic to $\mathbb{F}_q$. If the scheme $S \to A$ is smooth of relative dimension 2 we obtain an elliptic surface $\tilde{S} = S_{\overline{\mathbb{F}_q}}$ over the field $\overline{\mathbb{F}_q}$. The action of the Frobenius automorphism on the second ℓ-adic cohomology group $H^2_{et}(\tilde{S}, \mathbb{Q}_\ell)$, where $\ell \neq q$, gives rise to the characteristic polynomial of the automorphism. The computation of the characteristic polynomial involves point counting of $\mathbb{F}_{q^r}$-rational points on the surface $S_{\overline{\mathbb{F}_q}}$ up to some r. The Lefschetz fixed point formula allows us to compute the traces and the characteristic polynomials of the Frobenii. We apply [20, Proposition 6.2] to estimate the number of eigenvalues of the form $p\zeta$, for some root of unity ζ, which gives a sharp upper bound on the rank of the Néron-Severi group $NS(S_{\overline{\mathbb{F}_q}})$. To conclude the computations, we apply the Shioda-Tate formula to obtain the rank of the group $E(\overline{\mathbb{Q}}(t))$. The rank of $E(\mathbb{Q}(t))$ is equal to $rank\, E(\overline{\mathbb{Q}}(t)) - 1$, because only one generator of the free part of $E(\overline{\mathbb{Q}}(t))$ is not defined over $\mathbb{Q}(t)$.

2. Notation and preliminaries

Let S be the set of Pythagorean triples

$$S = \{(a,b,c) \in \mathbb{Z}^3 : a^2 + b^2 = c^2\}. \tag{2.1}$$

For each $s = (a,b,c) \in S$ we consider a curve over $\mathbb{Q}$

$$E_s : y^2 = x(x-a^2)(x-b^2). \tag{2.2}$$

When $ab(a^2-b^2) \neq 0$ the equation defines a non-singular curve of genus one, hence an elliptic curve. The discriminant of the equation E_s and its j-invariant are:

$$\Delta(s) = \Delta(a,b,c) = (16)(a-b)^2(a+b)^2b^4a^4. \tag{2.3}$$

$$j(s) = j(a,b,c) = 256 \cdot \frac{(a^4 - a^2b^2 + b^4)^3}{b^4a^4(a-b)^2(a+b)^2}. \tag{2.4}$$

Let $S_{\text{smooth}} = \{s \in S : \Delta(s) \neq 0\}$.

Let us now introduce the notion of equivalence of two tuples $s_1, s_2 \in S_{\text{smooth}}$. We call two such tuples equivalent if two smooth curves E_{s_1} and E_{s_2} are equivalent via a linear change of coordinates transforming one Weierstrass equation into another one. We will write it as $s_1 \sim s_2$. It is easy to check that $(a,b,c) \sim (A,B,C)$ if and only if there exists $u \in \mathbb{Q}^\times$ such that either $(a,b,c) = (\pm uA, \pm uB, \pm uC)$ or $(a,b,c) = (\pm uB, \pm uA, \pm uC)$. The relation $\sim$ is an equivalence

relation. Hence, if s_1 and s_2 do not lie in the same equivalence class, the associated elliptic curves E_{s_1} and E_{s_2} are non-isomorphic.

For any $s = (a, b, c) \in S_{\text{smooth}}$ we introduce a new parameter $t = t(s) = \frac{b}{c-a}$. It is well-defined because a triple with $a = c$ cannot lie in S_{smooth}. We have the following equalities:

$$\frac{t^2 - 1}{t^2 + 1} = \frac{a}{c}, \tag{2.5}$$

$$\frac{2t}{t^2 + 1} = \frac{b}{c}. \tag{2.6}$$

Define an elliptic curve over $\mathbb{Q}(t)$:

$$E_t : y^2 = x(x - (t^2 - 1)^2)(x - 4t^2). \tag{2.7}$$

A linear change of variables $x \mapsto x\frac{4}{(a-c)^2}, y \mapsto y\frac{8}{(c-a)^3}$ defines a $\mathbb{Q}$-isomorphism between elliptic curves $E_{(a,b,c)}$ and $E_{\frac{b}{c-a}}$ for any $(a, b, c) \in S_{\text{smooth}}$.

The discriminant and j-invariant of the curve E_t are

$$\Delta(t) = 256t^4 \left(-1 + t^2\right)^4 \left(1 - 6t^2 + t^4\right)^2,$$

$$j(t) = \frac{16\left(1 - 8t^2 + 30t^4 - 8t^6 + t^8\right)^3}{t^4\left(-1 + t^2\right)^4\left(1 - 6t^2 + t^4\right)^2}.$$

The set $P = \{t \in \mathbb{Q} : \Delta(t) \neq 0\} = \mathbb{Q} \setminus \{0, \pm 1\}$ consists of all parameters for which E_t is nonsingular. If $t \in P$, then E_t is $\mathbb{Q}$-isomorphic to a curve in Legendre form

$$y^2 = x\,(x - 1)\left(x - \left(\frac{2t}{t^2 - 1}\right)^2\right).$$

It is easy to check that two curves E_t and E_s are $\mathbb{Q}$-isomorphic if and only if

$$s \in \left\{t, -t, \frac{1}{t}, -\frac{1}{t}, \frac{1+t}{1-t}, \frac{1-t}{1+t}, -\frac{1-t}{1+t}, -\frac{1+t}{1-t}\right\}.$$

Rational functions in variable t, defined as above, form a group with composition. It is the dihedral group on 8 elements generated by two mappings: $f(t) = -t$ and $g(t) = \frac{1+t}{1-t}$. An equivalence relation can be defined on the set P where $s, t \in P$ are in relation $s \sim t$ can if and only if the curves E_t and E_s are $\mathbb{Q}$-isomorphic. Hence each equivalence class contains at most 8 different elements.

Consequently, we obtain the following

Proposition 2.1. There is a a bijection of sets of equivalence classes

$$S_{\text{smooth}}/\sim\to P/\sim \tag{2.8}$$

given by $(a, b, c) \mapsto \frac{b}{c-a}$ on representatives. The inverse is given by

$$\frac{p}{q} \mapsto (p^2 - q^2, 2pq, p^2 + q^2)$$

.

3. Elliptic surfaces and Picard numbers

We start this section by recalling all neccessary theorems and definitions related to elliptic surfaces. We compute Picard numbers of several elliptic surfaces and deduce the generic rank of the Mordell-Weil group of elliptic curves related to family (1.1).

Definition 3.1. Let k be an algebraically closed field. Let C be a smooth, irreducible, projective curve over k. An *elliptic surface over* C is a smooth, irreducible, projective surface S over k with a relatively minimal elliptic fibration $f : S \to C$ with a singular fiber and a zero section.

For an elliptic curve E over the function field $k(C)$ of the curve C we can associate an elliptic surface $f : \mathcal{E} \to C$ with generic fiber E. It follows from the work of Kodaira and Néron that f always exists and is unique. Further we refer to this elliptic surface as Kodaira-Néron model of an elliptic curve E over $k(C)$.

Below we define three different elliptic surfaces, starting from three distinguished elliptic curves over the function field of $\mathbb{P}^1$ over $\overline{\mathbb{Q}}$. Let $\mathcal{E}_1 \to \mathbb{P}^1$ be an elliptic surface over $\mathbb{P}^1$ associated to

$$y^2 = x(x-(t-1)^2)(x-4t).$$

Let $\mathcal{E}_2 \to \mathbb{P}^1$ be an elliptic surface over $\mathbb{P}^1$ associated to

$$y^2 = x(x-(t^2-1)^2)(x-4t^2).$$

Finally, let $\mathcal{E}_3 \to \mathbb{P}^1$ be an elliptic surface over $\mathbb{P}^1$ associated to

$$y^2 = x(x-(u^2-1)^2)(x-4u^2), \quad u = \frac{2t}{5+t^2}.$$

For any smooth, projective, geometrically integral variety V over a field K we denote by $NS(V_{\overline{K}})$ the Néron-Severi group, i.e. the group of divisors on V modulo algebraic equivalence.

Theorem 3.2 ([15], Corollary 2.2)**.** *Let $S \to C$ be an elliptic surface. The Néron-Severi group $NS(S)$ is finitely generated and torsion-free.*

Definition 3.3. Let $S \to C$ be an elliptic surface. The *Picard number* $\rho(S)$ of the surface S is the rank of the Néron-Severi group $NS(S)$.

We recall the classical the Shioda-Tate formula.

Theorem 3.4 ([15], Corollary 5.3)**.** *Let $S \to C$ be an elliptic surface. Let $R \subset C$ be the set of points under singular fibers. For each $v \in R$ let m_v denote the number of components of a singular fiber under v. Let E denote the generic fiber of S and K be the function field of C. Let $\rho(S)$ denote the rank of Néron-Severi group of S. We have the following identity*

$$\rho(S) = 2 + \sum_{v \in R}(m_v - 1) + rank(E(K)).$$

Lemma 3.5. *Let E be an elliptic curve over $\overline{\mathbb{Q}}(t)$. Let $\Sigma \subset \mathbb{P}^1(\overline{\mathbb{Q}})$ be the set of points of bad reduction of E. Let F_v denote the fibre at $v \in \Sigma$. We denote by $G(F_v)$ the group generated by simple components of F_v. There exists an injective homomorphism*

$$\phi : E\left(\overline{\mathbb{Q}}(t)\right)_{tors} \to \prod_{v \in \Sigma} G(F_v).$$

If F_v is of multiplicative type I_n in Kodaira notation (cf. [17, Theorem IV.8.2]*), the corresponding group is $\mathbb{Z}/n\mathbb{Z}$. If F_v is of additive type I_{2n}^*, the group is $(\mathbb{Z}/2\mathbb{Z})^2$.*

Proof. The map ϕ is a group homomorphism by [17, Theorem IV.9.2]. It is injective by [14, Corollary 7.5]. □

A multiplicative fiber of type I_n has exactly n components. An additive fiber of type I_{2n}^* has $5+2n$ components.

We gather the information about surfaces in Table 1, Table 2 and Table 3. We apply the Shioda-Tate formula to surfaces $\mathcal{E}_1, \mathcal{E}_2$ and $\mathcal{E}_3$.

Lemma 3.6.

(1) *Surface $\mathcal{E}_1$ is of Kodaira dimension $-\infty$.*
(2) *Surface $\mathcal{E}_2$ is of Kodaira dimension 0.*
(3) *Surface $\mathcal{E}_3$ is of Kodaira dimension 1.*

Proof. The Euler-Poincaré characteristic $e(S)$ of an elliptic surface $S \to C$ (over base field of characteristic different than 2 and 3) equals

$$e(S) = \sum_{v \in \Sigma} e(F_v),$$

where Σ is the set of points over which there are singular fibers. The local Euler number $e(F_v)$ is equal to the number of components m_v if the fiber has multiplicative reduction, or to $m_v + 1$ if the reduction is additive, cf. [4, Proposition 5.1.6]. An easy computation with the Tate algorithm (cf. Table 1, Table 2 and Table 3) shows that $e(\mathcal{E}_1) = 12$, $e(\mathcal{E}_2) = 24$ and $e(\mathcal{E}_3) = 48$. From [2, Corollary V.12.3] it follows that the Kodaira dimensions are: $\kappa(\mathcal{E}_1) = -\infty$, $\kappa(\mathcal{E}_2) = 0$ and $\kappa(\mathcal{E}_3) = 1$, respectively. □

Place	Type of singular fiber	Automorphism group
$t=1$	I_4	$\mathbb{Z}/4\mathbb{Z}$
$t=0$	I_2	$\mathbb{Z}/2\mathbb{Z}$
roots of $1-6t+t^2=0$	I_2	$\mathbb{Z}/2\mathbb{Z}$
$t=\infty$	I_2	$\mathbb{Z}/2\mathbb{Z}$

TABLE 1. Singular fibers, $E_1 : y^2 = x(x-(t-1)^2)(x-4t)$

place	Type of singular fiber	Automorphism group
$t=1$	I_4	$\mathbb{Z}/4\mathbb{Z}$
$t=0$	I_4	$\mathbb{Z}/4\mathbb{Z}$
$t=-1$	I_4	$\mathbb{Z}/4\mathbb{Z}$
roots of $-1-2t+t^2=0$	I_2	$\mathbb{Z}/2\mathbb{Z}$
roots of $-1+2t+t^2=0$	I_2	$\mathbb{Z}/2\mathbb{Z}$
$t=\infty$	I_4	$\mathbb{Z}/4\mathbb{Z}$

TABLE 2. Singular fibers, $E_2 : y^2 = x(x-(t^2-1)^2)(x-4t^2)$

The information gathered in Table 1, Table 2 and Table 3 allows us to prove the following results.

Lemma 3.7. *The generic fiber of $\mathcal{E}_1$ has rank 1 over $\overline{\mathbb{Q}}(t)$.*

Proof. The surface $\mathcal{E}_1$ is rational by Lemma 3.6, hence $\rho(\mathcal{E}_1) = 10$. A section of $\mathcal{E}_1$ corresponds to a point on the generic fiber

$$P = (-4t, 4\sqrt{-2}t(t+1)). \tag{3.1}$$

Place	Type of singular fiber	Automorphism group
$t=0$	I_4	$\mathbb{Z}/4\mathbb{Z}$
roots of $5+t^2=0$	I_4	$\mathbb{Z}/4\mathbb{Z}$
roots of $5-2t+t^2=0$	I_4	$\mathbb{Z}/4\mathbb{Z}$
roots of $5+2t+t^2=0$	I_4	$\mathbb{Z}/4\mathbb{Z}$
roots of $25-20t+6t^2-4t^3+t^4=0$	I_2	$\mathbb{Z}/2\mathbb{Z}$
roots of $25+20t+6t^2+4t^3+t^4=0$	I_2	$\mathbb{Z}/2\mathbb{Z}$
$t=\infty$	I_4	$\mathbb{Z}/4\mathbb{Z}$

TABLE 3. Singular fibers, $E_3 : y^2 = x(x-(u^2-1)^2)(x-4u^2)$, $u=\frac{2t}{5+t^2}$

As $2P$ and $4P$ are not zero, the point is non-torsion by Lemma 3.5. The group $E_1(\overline{\mathbb{Q}}(t))$ is at least of rank 1. By applying the Shioda-Tate formula we get

$$\rho(\mathcal{E}_1) - 2 - \sum_{v\in R}(m_v - 1) = rank(E_1(\overline{\mathbb{Q}}(t)))$$

$$\rho(\mathcal{E}_1) - 2 - \sum_{v\in R}(m_v - 1) = 10 - 2 - (4-1+4(2-1)) = 10-2-7 = 1.$$

Hence the rank equals 1. □

Lemma 3.8. *The generic fiber of $\mathcal{E}_2$ has rank 2 over $\overline{\mathbb{Q}}(t)$.*

Proof. The surface is $K3$ so $\rho(\mathcal{E}_2) \leq 20$. Let us find two points of infinite order

$$P = (-4t^2, 4\sqrt{-2}t^2(t^2+1)),$$
$$Q = (2(t-1)^2, 2(-1+t)^2(-1+2t+t^2)).$$

We compute the height pairing $\langle P,P\rangle = 2$, $\langle Q,Q\rangle = 1$ and $\langle P,Q\rangle = 0$. Application of the Shioda-Tate formula shows that

$$20 \geq \rho(\mathcal{E}_2) = 2 + (4(4-1)+4(2-1)) + rank(E_2(\overline{\mathbb{Q}}(t)) = 18 + rank(E_2(\overline{\mathbb{Q}}(t)).$$

Hence the rank is equal to two. □

Application of the Shioda-Tate formula allows us to conclude that the Mordell-Weil group of $\overline{\mathbb{Q}}(t)$-rational points of the generic fiber of $\mathcal{E}_3$ has rank at most 6. More precisely, $\rho(\mathcal{E}_3) \leq 40$ (since $\chi(\mathcal{O}_{\mathcal{E}_3}) = 4$) and

$$2 + \sum_{v\in R}(m_v - 1) = 2 + 8(4-1) + 8(2-1) = 2+24+8 = 34.$$

There are only three sections of infinite order which are linearly independent.

Let X be any scheme over a finite field $\mathbb{F}_q$ of characteristic p. Let $\ell \neq p$ be a prime. Let us consider étale cohomology groups with the Tate twist $H^i_{\text{ét}}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l)(m)$, which we denote for simplicity by $H^i(X, \mathbb{Q}_l)(m)$.

Theorem 3.9 ([20], Proposition 6.2)**.** *Let A be a discrete valuation ring of a number field L with the residue field $k \cong \mathbb{F}_q$. Let S be an integral scheme with a morphism $S \to Spec\, A$ that is projective and smooth of relative dimension 2. Let us assume that the surfaces $\overline{S} = S_{\overline{L}}$ and $\tilde{S} = S_{\overline{k}}$ are integral. Let $l \nmid q$ be a prime number. Then there are natural injective homomorphisms*

$$NS(\overline{S}) \otimes \mathbb{Q}_l \hookrightarrow NS(\tilde{S}) \otimes \mathbb{Q}_l \hookrightarrow H^2_{ét}(\tilde{S}, \mathbb{Q}_l)(1) \tag{3.2}$$

of finite dimensional inner product spaces over $\mathbb{Q}_l$*. The first injection is induced by the natural injection* $NS(\overline{S})\otimes\mathbb{Q}\hookrightarrow NS(\tilde{S})\otimes\mathbb{Q}$*. The second injection respects the Galois action of* $G(\overline{k}/k)$*.*

For any prime p and any positive integer r and a variety X over $\mathbb{F}_{p^r}$ we denote by $F_X : X \to X$ the absolute Frobenius morphism which acts as the identity on points and as $f \mapsto f^p$ on the structure sheaf. Let $\Phi_X = (F_X)^r$ and $\overline{X} = X_{\overline{\mathbb{F}}_{p^r}}$ and we denote by $\Phi_X \times 1$ the morphism which acts on $Z \times Spec\overline{\mathbb{F}}_{p^r}$. This induces an automorphism Φ_X^* of $H^i_{\text{ét}}(\overline{X}, \mathbb{Q}_l)$.

Theorem 3.10 ([20], Corollary 2.3)**.** *With notation as in the previous theorem, the ranks of* $NS(\overline{S})$ *and* $NS(\tilde{S})$ *are bounded from above by the number of eigenvalues of the linear map* $\Phi^*_{\tilde{S}}$ *for which* λ/q *is a root of unity, counted with multiplicity.*

To be able to use the above theorem effectively, we recall the Lefschetz trace formula, cf. [10, VI, Theorem 12.3].

Theorem 3.11. *Let* X *be a smooth projective variety over* $\mathbb{F}_q$ *of dimension* n*. For any prime* $l \nmid q$ *and any integer* m*, we have*

$$\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{n}(-1)^i Tr((\Phi_X^*)^m \mid H^i(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l)).$$

We explain the use of the Lefschetz trace formula in numerical computation of the characteristic polynomial of the Frobenius automorphism, which we apply in the proofs of Lemma 4.8 and Lemma 5.4 below. We proceed with $X = S_{\overline{\mathbb{F}_q}}$, an elliptic surface fibered over $\mathbb{P}^1$. Note that $\dim H^1(X,\mathbb{Q}_l) = \dim H^3(X,\mathbb{Q}_l)$ by [7, Corollary 2A10] and $\dim H^1(X,\mathbb{Q}_l) = 0$ by [4, Corollary 5.2.2]. Automorphism Φ_X^* acts on $H^4(X,\mathbb{Q}_l) = \mathbb{Q}_l$ by multiplication by q^2. By the Lefschetz trace formula we obtain

$$Tr((\Phi_X^*)^m \mid H^2(X,\mathbb{Q}_l)) = \#X(\mathbb{F}_{q^m}) - 1 - q^{2m}.$$

Let V be a linear subspace of $H^2(X,\mathbb{Q}_l)$ generated by components of singular fibers and sections. Let $W = H^2(X,\mathbb{Q}_l)/V$. By the multiplicativity of the characteristic polynomial $char(\Phi_X^*)$ we have that

$$char(\Phi_X^*) = char(\Phi_X^*|V)\cdot char(\Phi_{X,W}^*)$$

where the operator $\Phi_{X,W}^* : W \to W$ is induced by Φ_X^*. Moreover,

$$Tr((\Phi_X^*)^m) = Tr((\Phi_X^*|V)^m) + Tr((\Phi_{X,W}^*)^m)$$

for any n. For T a linear operator acting on a finite dimensional vector space U, the characteristic polynomial $p(x) = \det(I\cdot x - T)$ can be computed if the traces $t_n = Tr(T^n)$ are known for $0 \le n \le \dim U$. In order to do that, we expand

$$p(x) = \frac{x^{\dim U}}{exp(\sum_{r=1}^{\infty} t_r \frac{x^{-r}}{r})} \tag{3.3}$$

as a series of $\frac{1}{x}$ and truncate the series to the polynomial part. In numerical computations below, we put $T = \Phi_X^*$.

4. Twisted elliptic surfaces

Now we prove that the rank of the Mordell-Weil group over $\overline{\mathbb{Q}}(t)$ of the elliptic curve

$$y^2 = x(x-(u^2-1)^2)(x-4u^2)$$

for $u = \frac{2t}{5+t^2}$ is equal to 3. For this purpose the notion of a twist of an elliptic curve is needed. In this section we use the approach from the paper [8] by Remke Kloosterman. We assume that

the base curve C of the elliptic fibration $\mathcal{E} \to C$ is defined over a field of characteristic not equal to 2 or 3.

Definition 4.1. Let C be a smooth curve over $k = \overline{k}$, and let $k(C)$ be the function field of C. Let E be an elliptic curve over $k(C)$ given by the Weierstrass equation

$$E : y^2 = x^3 + Ax + B \tag{4.1}$$

for $A, B \in k(C)$. Let us fix an element $u \in k(C)^*$. The elliptic curve

$$E^{(u)} : uy^2 = x^3 + Ax + B$$

is called the twist of the curve E by the element u.

Proposition 4.2. With the above notation the following equality holds

$$rank\, E(k(C)) + rank\, E^{(u)}(k(C)) = rank\, E(k(C)(\sqrt{u})).$$

Proof. See [16, Exercise 10.16]. □

Definition 4.3. Let $f : \mathcal{E} \to C$ be an elliptic surface. Fix two points $P, Q \in C(k)$. Let $E/k(C)$ be the generic fiber of f given by the Weierstrass equation (4.1). An elliptic surface $g : \mathcal{E}' \to C$ *is the twist of f by points P and Q* if the generic fiber of g is isomorphic over $k(C)$ to $E^{(u)}$, where $u \in k(C)^*$ and the function u satisfies the following properties of the valuations:

$$\mathrm{ord}_P(u) \equiv 1 \bmod 2$$

and

$$\mathrm{ord}_Q(u) \equiv 1 \bmod 2.$$

In addition, we require that for all $R \notin P, Q$

$$\mathrm{ord}_R(u) \equiv 0 \bmod 2.$$

Remark 4.4. For any pair of points P and Q we form a divisor $(P) - (Q) \in \mathrm{Div}^0(C)$. The group of k-rational points of the Jacobian $\mathrm{Jac}(C)$ of the curve C equals $\mathrm{Pic}^0(C)$. Since k is algebraically closed, the group $\mathrm{Pic}^0(C)$ is 2-divisible. We find that $(P) - (Q) = 2D + \mathrm{div}(f)$ for a function $f \in k(C)^*$ and $D \in \mathrm{Div}^0(C)$. We put $u := f$. Let u' be another function such that $\mathrm{div}(u') \equiv (P) - (Q) \bmod 2\mathrm{Div}^0(C)$. The twists $E^{(u)}$ and $E^{(u')}$ may not be isomorphic over $k(C)$. We have $\mathrm{div}(\frac{u}{u'}) = 2T$ for some divisor $T \in \mathrm{Div}^0(C)$. If the genus g of C is greater than 0, then $T \in \mathrm{Jac}(C)(k)$ is a 2-torsion point. There are 2^{2g} distinct torsion points in $\mathrm{Jac}(C)(k)$, hence there are 2^{2g} distinct twists by points P, Q, up to a $k(C)$-isomorphism. However, for $C = \mathbb{P}^1$, a pair of points P, Q determines a twist uniquely.

Lemma 4.5. *Let $f : \mathcal{E} \to C$ be an elliptic surface and let $f^{(P,Q)} : \mathcal{E}^{(P,Q)} \to C$ be the twist by $P, Q \in C(k)$. There exists a double cover $\phi : C' \to C$ ramified at P and Q such that the relatively minimal nonsingular models of $\mathcal{E} \times_C C' \to C'$ and $\mathcal{E}^{(P,Q)} \times_C C' \to C'$ are isomorphic as fibered surfaces.*

Proof. Let E denote the generic fiber of the elliptic fibration f. Let u be the function in $k(C)$ satisfying the conditions of Definition 4.3 for the points P and Q in $C(k)$. The generic fiber of $f^{(P,Q)}$ is the twist $E^{(u)}$ of the curve E.

There exists a projective curve C' and a surjective morphism $\phi : C' \to C$ such that $u \circ \phi = v^2$ for some element $v \in k(C')$. We denote by $e_\phi(R)$ the ramification index of the morphism ϕ at the point R in the fiber above the point $\phi(R) \in C(k)$. By definition, the function u has a divisor $div(u) = (P) + (Q) + 2D$ for some $D \in Div(C)$. Hence

$$div(u \circ \phi) = \phi^*(div\, u) = \sum_{R \in \phi^{-1}(P)} e_\phi(R)(R) + \sum_{R' \in \phi^{-1}(Q)} e_\phi(R')(R') + \phi^* D = 2\, div\, v, \tag{4.2}$$

where $\phi^* : Div(C) \to Div(C')$ denotes the induced map. The extension $k(C')$ of $k(C)$ is of degree 2, so

$$2 = deg\,\phi = \sum_{R \in \phi^{-1}(P)} e_\phi(R) = \sum_{R' \in \phi^{-1}(Q)} e_\phi(R'). \tag{4.3}$$

Identities (4.2) and (4.3) imply that ϕ is ramified at P and Q and the preimages $\phi^{-1}(P)$ and $\phi^{-1}(Q)$ are singletons.

Let $S_1 = \mathcal{E} \times_C C'$ and $S_2 = \mathcal{E}^{(P,Q)} \times_C C'$ denote the surfaces obtained from $\mathcal{E}$ and $\mathcal{E}^{(P,Q)}$ by the base change $\phi : C' \to C$. The morphisms f and $f^{(P,Q)}$ are projective, hence $S_1 \to C'$ and $S_2 \to C'$ are projective. As the base field k is algebraically closed, all but finitely many fibers of $S_1 \to C'$ and $S_2 \to C'$ are nonsingular elliptic. Let $\tilde{S_1}$ denote a relatively minimal nonsingular model of S_1, respecting the fibration over C'. Similarly, let $\tilde{S_2}$ denote the relatively minimal nonsingular model of S_2. By a linear change of coordinates, the generic fibers E and $E^{(u)}$ are isomorphic over $k(C')$. This implies that there is a birational map $\psi : \tilde{S_1} \dashrightarrow \tilde{S_2}$. Each such map is a composition of smooth blow-ups and blow-downs. The desingularizations $\tilde{S_1}$ and $\tilde{S_2}$ are isomorphic outside the singular fibers. The surfaces $\tilde{S_1}$ and $\tilde{S_2}$ are relatively minimal with respect to C', so the fibers do not contain (-1)-curves. Hence, the map ψ is a trivial composition, hence extends to an isomorphism. $\square$

We introduce the following elliptic surfaces which will be used in the computation of ranks of the families associated to Pythagorean triples, cf. proofs of Theorem 1.1, 1.3.

Definition 4.6.

(1) Let $\mathcal{E}_1 \to \mathbb{P}^1$ be the elliptic surface with the generic fiber
$$E_1 : y^2 = x(x-(t-1)^2)(x-4t).$$

(2) We denote by $\mathcal{E}_1' = \mathcal{E}_1^{(\frac{1}{5},\infty)} \to \mathbb{P}^1$ the twist of $\mathcal{E}_1$ by the points $\frac{1}{5}$ and ∞, which has the generic fiber
$$E_1' : -(-1+5t)y^2 = x(x-(t-1)^2)(x-4t).$$

(3) We denote by $\mathcal{E}_1'' = (\mathcal{E}_1')^{(0,\infty)} \to \mathbb{P}^1$ the twist of $\mathcal{E}_1'$ by the points 0 and ∞, which has the generic fiber
$$E_1'' : -t(-1+5t)y^2 = x(x-(t-1)^2)(x-4t).$$

(4) Let $\mathcal{E}_2 \to \mathbb{P}^1$ be the elliptic surface with the generic fiber
$$E_2 : y^2 = x(x-(t^2-1)^2)(x-4t^2).$$

(5) We denote by $\mathcal{E}_2' = \mathcal{E}_2^{(\frac{-1}{\sqrt{5}},\frac{1}{\sqrt{5}})} \to \mathbb{P}^1$ the twist of $\mathcal{E}_2$ by the points $\frac{-1}{\sqrt{5}}$ and $\frac{1}{\sqrt{5}}$, which has the generic fiber
$$E_2' : -(-1+5t^2)y^2 = x(x-(t^2-1)^2)(x-4t^2).$$

(6) Let $\mathcal{E}_3 \to \mathbb{P}^1$ be the elliptic surface which has the generic fiber
$$E_3 : y^2 = x(x-((\frac{2t}{5+t^2})^2-1)^2)(x-4(\frac{2t}{5+t^2})^2).$$

Proposition 4.2 implies the following statement.

Corollary 4.7. *The following equalities hold*
$$rank\, E_3(\overline{\mathbb{Q}}(t)) = rank\, E_2(\overline{\mathbb{Q}}(t)) + rank\, E_2'(\overline{\mathbb{Q}}(t)),$$
$$rank\, E_2'(\overline{\mathbb{Q}}(t)) = rank\, E_1'(\overline{\mathbb{Q}}(t)) + rank\, E_1''(\overline{\mathbb{Q}}(t)),$$

Lemma 4.8. *The rank of $E_1'(\overline{\mathbb{Q}}(t))$ is equal to 0.*

Proof. First we perform the Tate algorithm to compute the types of singular fibers on our elliptic surface $\mathcal{E}_1^{'} \to \mathbb{P}^1$ associated with the curve $E_1^{'}$. A computation in MAGMA reveals that we have one fiber over the point $t = 1$ of multiplicative type I_4, split over $\mathbb{Q}$. One singular fiber lies above $t = 0$ and is non-split multiplicative of type I_2, nonetheless the equations are defined over $\mathbb{Q}$. We have a fiber over $t = \frac{1}{5}$, additive of type I_0^* and again by the Tate algorithm and MAGMA the defining equations of the fiber have coefficents in $\mathbb{Q}$. The singular fiber over $t = \infty$ is additive of the type I_2^* given by equations with coefficients in $\mathbb{Q}$. Finally, we have two singular fibers of non-split multiplicative type I_2 above $t = 3 + 2\sqrt{2}$ and $t = 3 - 2\sqrt{2}$. The equations of the fibers are defined over $\mathbb{Q}(\sqrt{2})$ by the Tate algorithm. However, the surface $\mathcal{E}_1^{'}$ is defined over $\mathbb{Q}$, since we have started with the Weierstrass equation of the elliptic curve $E_1^{'}$ defined over $\mathbb{Q}$ and the singular locus defines an ideal where the generators have $\mathbb{Q}$-coefficients. In fact, $\mathcal{E}_1^{'}$ is defined over $\mathbb{Z}$. We check that the elliptic surface associated with $E_1^{'}$ over $\mathbb{F}_{17}$ has the types of singular fibers above the reductions of points $t = 1, 0, \infty, 3 \pm 2\sqrt{2}$ the same as in characteristic zero. Put $\mathfrak{p} = (17) \in Spec\,\mathbb{Z}$ and $A = \mathbb{Z}_{(\mathfrak{p})}$. The surface $\mathcal{E}_1^{'}$ defines an integral scheme $S \to Spec\,A$ that is projective and smooth of relative dimension 2. The smoothness comes from the fact that we have a good reduction at 17. The residue field $k = A/\mathfrak{p}$ is equal to $\mathbb{F}_{17}$. Hence, the special fiber of $S \to Spec\,A$ is a surface defined over $\mathbb{F}_{17}$. It determines an elliptic surface $\tilde{S} = S_{\overline{\mathbb{F}_{17}}} \to \mathbb{P}^1$ which is the reduction of our elliptic surface $\mathcal{E}_1^{'} \to \mathbb{P}^1$. By Theorem 3.9 we know that the rank of the Néron-Severi group of $\mathcal{E}_1^{'}$ is bounded from above by the rank of the Néron-Severi group of $\tilde{S}$. Components of the singular fibers and the zero section generate a rank 18 subgroup in $NS(\tilde{S})$. The Euler-Poincaré characteristic $e(\mathcal{E}_1^{'})$ equals 24 as follows by an argument based on the proof of Lemma 3.6. Hence, the surface $\mathcal{E}_1^{'}$ is $K3$. Good reduction at prime 17 implies that also $\tilde{S}$ is a $K3$ surface, so the subspace $NS(\tilde{S}) \otimes \mathbb{Q}_\ell \hookrightarrow H^2_{\text{ét}}(\tilde{S}, \mathbb{Q}_\ell)(1)$ is at most of dimension 22, because $\dim_{\mathbb{Q}_\ell} H^2_{\text{ét}}(\tilde{S}, \mathbb{Q}_\ell)(1) = \dim_{\mathbb{Q}_\ell} H^2_{\text{ét}}(\tilde{S}, \mathbb{Q}_\ell) = 22$ by [12, Theorem 4, Part III]. On the subspace V generated by components of singular fibers and by zero section the Frobenius automorphism $\Phi^*_{\tilde{S}}$ acts by multiplication by 17. It follows from the analysis of the singular fibers, i.e. by the Tate algorithm. The characteristic polynomial of the Frobenius automorphism $\Phi^*_{\tilde{S}}$ splits as follows

$$char(\Phi^*_{\tilde{S}}) = char(\Phi^*_{\tilde{S}} \mid V) \cdot char(\Phi^*_{\tilde{S}, H^2_{\text{ét}}/V}).$$

Then $char(\Phi^*_{\tilde{S}} \mid V) = \det(Id \cdot x - \Phi^*_{\tilde{S}} \mid V) = (x - 17)^{18}$. For any natural m an equality holds

$$Tr((\Phi^*_{\tilde{S}})^m) = Tr((\Phi^*_{\tilde{S}} \mid V)^m) + Tr((\Phi^*_{\tilde{S}, H^2_{\text{ét}}/V})^m).$$

But we have $Tr((\Phi^*_{\tilde{S}} \mid V)^m) = 18 \cdot 17^m$ and $Tr((\Phi^*_{\tilde{S}, H^2_{\text{ét}}/V})^m) = \#\tilde{S}(\mathbb{F}_{17^m}) - 1 - 17^{2m}$ by Lefschetz trace formula (cf. Theorem 3.11). Combining those facts we obtain

$$Tr((\Phi^*_{\tilde{S}, H^2_{\text{ét}}/V})^m) = \#\tilde{S}(\mathbb{F}_{17^m}) - 1 - 17^{2m} - 18 \cdot 17^m.$$

The characteristic polynomial $char(\Phi^*_{\tilde{S}, H^2_{\text{ét}}/V})$ is of the form $x^4 + c_1 x^3 + c_2 x^2 + c_3 x + c_4$. We present explicit formulas for c_m in terms of $t_m = Tr((\Phi^*_{\tilde{S}, H^2_{\text{ét}}/V})^m)$ (cf. equation (3.3))

$$\begin{aligned}
c_1 &= -t_1 \\
c_2 &= \frac{1}{2}(t_1^2 - t_2) \\
c_3 &= \frac{1}{6}(-t_1^3 + 3t_1 t_2 - 2t_3) \\
c_4 &= \frac{1}{24}(t_1^4 - 6t_1^2 t_2 + 3t_2^2 + 8t_1 t_3 - 6t_4)
\end{aligned}$$

We compute the number of $\mathbb{F}_{17^m}$-rational points on $\tilde{S}$ up to $m=4$.

m	1	2	3	4
$\#\tilde{S}(\mathbb{F}_{17^m})$	604	88312	24227740	6977057176

We obtain the characteristic polynomial $char(\Phi^*_{\tilde{S},H^2_{\acute{e}t}/V}) = x^4-8x^3+238x^2-2312x+83521$. Suppose a root of this polynomial is $x=17\zeta$ for some root of unity ζ. Then

$$4913(17\zeta^4-8\zeta^3+14\zeta^2-8\zeta+17)=0.$$

But ζ is an algebraic integer and the polynomial $17x^4-8x^3+14x^2-8x+17$ is irreducible over $\mathbb{Q}$, hence its roots are not algebraic integers, which leads to a contradiction. Hence, the characteristic polynomial $char(\Phi^*_{\tilde{S}}) = (x-17)^{18}(x^4-8x^3+238x^2-2312x+83521)$ has only 18 roots of the shape 17 times a root of unity. By Theorem 3.10 the rank of $NS(\tilde{S})$ is at most 18. Then by Theorem 3.9 the rank of $NS(\mathcal{E}_1')$ is equal to 18 since we have an explicit rank 18 subgroup generated by singular fibers components and the zero section. By the Shioda-Tate formula the rank of $E_1'(\overline{\mathbb{Q}}(t))$ equals zero. □

5. Computing ranks by reductions

Let p be a prime of good reduction for an elliptic surface $\mathcal{E}\to C$ defined over a number field K. Let S be an integral model of $\mathcal{E}$ over $\mathcal{O}_K$ with special fiber defined over $\mathbb{F}_{p^r}$. We know by Theorem 3.9 that

$$NS(S_{\overline{\mathbb{Q}}})\otimes\mathbb{Q}\hookrightarrow NS(S_{\overline{\mathbb{F}}_{p^r}})\otimes\mathbb{Q}.$$

Assume for a moment that the map is an isomorphism. Then by classical results in lattice theory it follows that the determinants of the Gram matrices of the intersection pairings on $NS(S_{\overline{\mathbb{Q}}})$ and $NS(S_{\overline{\mathbb{F}}_{p^r}})$ differ by a square. In the sequel, we denote the determinant of the Gram matrix of a lattice Λ by $\Delta(\Lambda)$.

We will compute discriminants modulo squares using the Tate conjecture and the Artin-Tate conjecture for K3 surfaces which we recall for the reader's convenience.

Theorem 5.1. *Let Y be a K3 surface over $\mathbb{F}_q$. Let Φ^*_Y be the Frobenius automorphism acting on the cohomology group $H^2(Y,\mathbb{Q}_l))$, $l\nmid q$. The number of roots of the characteristic polynomial of Φ^*_Y of the form $q\zeta$, where ζ is a root of unity is equal to the Picard number $\rho(Y) = rank\,NS(Y_{\overline{\mathbb{F}}_q})$.*

Theorem 5.2. *Let Y be a K3 surface over $\mathbb{F}_q$. Let Φ^*_Y be the Frobenius automorphism and $P(T)=\det(1-T\Phi^*_Y|H^2(Y,\mathbb{Q}_l))$. Then*

$$\lim_{s\to1}\frac{P(q^{-s})}{(1-q^{1-s})^{\rho'(Y)}} = \frac{(-1)^{\rho'(Y)-1}\sharp Br(Y)\Delta(NS(Y_{\mathbb{F}_q}))}{q^{\alpha(Y)}(\sharp NS(Y_{\mathbb{F}_q})_{tor})^2},$$

where $\alpha(Y)=\chi(Y,\mathcal{O}_Y)-1+\dim Pic^0(Y)$ and $Br(Y)$ is the Brauer group of Y. Moreover $\rho'(Y) = rank\,NS(Y_{\mathbb{F}_q})$. The group $NS(Y_{\mathbb{F}_q})$ is the subgroup of the Néron-Severi group $NS(Y_{\overline{\mathbb{F}}_q})$ generated by $\mathbb{F}_q$-rational divisors.

Tate conjectures for elliptic $K3$ surfaces are proven in [1, Theorem 5.2]. J. S. Milne proved that the Tate conjectures imply the Artin-Tate conjectures for characteristic different than 2, cf. [9, Theorem 6.1]. Finally, in [11, Theorem 0.4b] the assumption on the characteristic was dropped.

Proposition 5.3 (Proposition 4.7,[8])**.** Suppose q is a prime power. Let $Y\to\mathbb{P}^1$ be an elliptic K3 surface, defined over $\mathbb{F}_q$. Assume that q is a square and that $\rho(Y)=\rho'(Y)$. Then

$$\Delta(NS(Y_{\overline{\mathbb{F}}_q})) \equiv -\lim_{s\to1}\frac{P(q^{-s})}{(1-q^{1-s})^{\rho(Y)}} \mod (\mathbb{Q}^*)^2.$$

Lemma 5.4. *The rank of* $E_1''(\overline{\mathbb{Q}}(t))$ *is equal to* 1.

Proof. It is easy to check that the point $Q = (1-t, 1-t)$ lies in $E_1''(\overline{\mathbb{Q}}(t))$ and that it is a point of infinite order. The configuration of singular fibers is given in Table 4. It follows by Lemma

place	Type of singular fiber	Automorphism group
$t=1$	I_4	$\mathbb{Z}/4\mathbb{Z}$
$t=\infty$	I_2	$\mathbb{Z}/2\mathbb{Z}$
$t=0$	I_2^*	$(\mathbb{Z}/2\mathbb{Z})^2$
$t=\frac{1}{5}$	I_0^*	$(\mathbb{Z}/2\mathbb{Z})^2$
$t=3+\sqrt{2}$	I_2	$(\mathbb{Z}/2\mathbb{Z})$
$t=3-\sqrt{2}$	I_2	$(\mathbb{Z}/2\mathbb{Z})$

TABLE 4. Singular fibers, $E_1'' : -t(-1+5t)y^2 = x(x-(t-1)^2)(x-4t)$

3.5 that it is enough to check that $2Q$ and $4Q$ are non-zero. The Euler characteristic $e(\mathcal{E}_1'') = 24$, which shows that $\mathcal{E}_1''$ is a $K3$ surface (cf. Table 4). Surface $\mathcal{E}_1^{''}$ is defined over $\mathbb{Z}$ (cf. proof of Lemma 4.8). We have two primes of good reduction 11 and 17. Consider the reduction of $\mathcal{E}_1^{''}$ at 11, which we denote by S_{11}. It is a K3 surface defined over $\mathbb{F}_{11}$. We have also a K3 surface obtained by the reduction at 17. We denote it by S_{17}. Note that it is defined over $\mathbb{F}_{17}$. Since we are interested only in the surfaces defined over $\mathbb{F}_{11^2}$ and $\mathbb{F}_{17^2}$, we will denote by S_{11} and S_{17} the base change of original surfaces to $\mathbb{F}_{11^2}$ and $\mathbb{F}_{17^2}$, respectively.

By an argument similar to the proof of Lemma 4.8 we compute the characteristic polynomials of the Frobenius automorphism acting on the second ℓ-adic cohomology group for some auxiliary prime $\ell \neq 11, 17$.

For $p = 11$ using MAGMA we get

$$char(\Phi^*_{S_{11}}) = (x-11^2)^{20}(x^2 - 158x + 14641).$$

Roots of the polynomial $x^2 - 158x + 14641$ are not of the form $11^2\zeta$, for some root of unity ζ. The rank of $NS((S_{11})_{\overline{\mathbb{F}}_{11^2}})$ equals 20 by Tate conjectures for K3 surfaces (cf. Theorem 5.1) For $p = 17$ we get

$$char(\Phi^*_{S_{17}}) = (x-17^2)^{20}(x^2 + 94x + 83521).$$

Roots of the polynomial $x^2 + 94x + 83521$ are not of the form $17^2\zeta$, for some root of unity ζ. Hence, the rank of $NS((S_{17})_{\overline{\mathbb{F}}_{17^2}})$ equals 20 by Tate conjectures for K3 surfaces. The rank of $NS((\mathcal{E}_1^{''})_{\overline{\mathbb{Q}}})$ is always smaller or equal to the rank of the corresponding Néron-Severi group after reduction (cf. Theorem 3.9). Assume for a moment that it is maximal possible, hence equal to 20. This implies that the discriminants of lattices $NS((S_{11})_{\overline{\mathbb{F}}_{11^2}})$ and $NS((S_{17})_{\overline{\mathbb{F}}_{17^2}})$ should differ by a square. We apply Theorem 5.2 to compute the discriminant of the Néron-Severi lattices $NS(\tilde{S}_{\overline{\mathbb{F}}_{17^2}})$ and $NS((S_{11})_{\overline{\mathbb{F}}_{11^2}})$. They are not equal modulo squares, more precisely we have

$$\Delta(NS((S_{11})_{\overline{\mathbb{F}}_{11^2}})) \equiv -3 \cdot 7 \bmod (\mathbb{Q}^*)^2$$

and

$$\Delta(NS((S_{17})_{\overline{\mathbb{F}}_{17^2}})) \equiv -2 \cdot 3 \cdot 7 \bmod (\mathbb{Q}^*)^2.$$

So the rank of $NS((\mathcal{E}_1^{''})_{\overline{\mathbb{Q}}})$ is less or equal to 19. Note that the trivial sublattice generated by components of singular fibers and the zero section is of rank 18. We also have the point Q of infinite order, so $19 \leq rank\, NS((\mathcal{E}_1^{''})_{\overline{\mathbb{Q}}})$. But the upper bound is also 19, hence the rank equals 19. Now an application of the Shioda-Tate formula reveals that the rank of $E_1''(\overline{Q}(t))$ is equal to 1. $\square$

Corollary 5.5. *The rank of* $E_3(\overline{\mathbb{Q}}(t))$ *is equal to* 3.

Proof. We apply Lemma 4.7 to ranks obtained in Lemma 4.8, Lemma 5.4 and Lemma 3.8. $\square$

Remark 5.6. One could give a more direct proof of Corollary 5.5 using brute force and more powerful numerical computations. The statement of Corollary 5.5 is equivalent to $\rho((\mathcal{E}_3)_{\overline{\mathbb{Q}}}) = 37$ by the Shioda-Tate formula (cf. Table 3 to compute the number of components in singular fibers). Suppose to the contrary that $\rho((\mathcal{E}_3)_{\overline{\mathbb{Q}}}) \geq 38$. This lower bound holds for the Néron-Severi group of the reduced elliptic surface at primes of good reduction. Suppose we have two such primes p_1 and p_2. Prime 17 is a good candidate, with the characteristic polynomial of the Frobenius automorphism (acting on the second cohomology group) equal to

$$(t+17)^8(t-17)^{30}(289-22t+t^2)(289-2t+t^2)(83521-2312t+238t^2-8t^3+t^4).$$

To compute the degree 8 factor we need to work with surfaces with points in the field $\mathbb{F}_{17^8}$ or $\mathbb{F}_{17^4}$ which follows by the Poincaré duality. None of the roots of

$$(289-22t+t^2)(289-2t+t^2)(83521-2312t+238t^2-8t^3+t^4)$$

are of the shape 17ζ for ζ a root of unity. Note that the Tate conjecture holds automatically for such a prime. By the results of J. S. Milne, cf. [9, Theorem 6.1] the Artin-Tate conjecture holds as well. Put $p_1 = 17$ and assume we have another such prime p_2. This means that we can compare the discriminants of the lattices modulo squares and arrive at a contradiction, which proves that $\rho((\mathcal{E}_3)_{\overline{\mathbb{Q}}}) = 37$. Using the method of twists and further computation other good primes can be found, namely 73 and 97 but no other up to 140. However, a direct computation of the points on surfaces over $\mathbb{F}_{73^4}$ or $\mathbb{F}_{97^4}$ is beyond the range of our computational resources.

6. Proofs of main results

Lemma 6.1. *The torsion subgroup of* $E_3(\overline{\mathbb{Q}}(t))$ *is isomorphic to* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. *It is generated by points*

$$T_1 = (-4u^2, 0)$$
$$T_2 = (2(-u+u^3), 2\sqrt{-1}(u^2-1)u(-1-2u+u^2)),$$

where $u = \frac{2t}{5+t^2}$.

Proof. Let $K = \overline{\mathbb{Q}}(t)$. The elliptic surface associated to E_3 has singular fibers of types I_2 and I_4 (cf. Table 3), hence

$$E_3(K)_{tors} \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^a \oplus (\mathbb{Z}/4\mathbb{Z})^b$$

for some natural numbers a and b by Lemma 3.5. The 2-torsion subgroup is generated by T_1 and $(0,0)$. We will check that $T_1 \notin 2E_3(K)$ and that $T_1 + (0,0) \notin 2E_3(K)$, but $(0,0) \in 2E_3(K)$.

Let $P = (x, y)$ be any point in $E_3(K)$. Then the x-coordinate of $2P$ is equal to

$$x(2P) = \frac{\left(4u^2 - 8u^4 + 4u^6 - x^2\right)^2}{4\left(4u^2 - x\right)\left(1 - 2u^2 + u^4 - x\right)x},$$

where $u = \frac{2t}{5+t^2}$. If T_1 were in $2E_3(K)$, then

$$x(2P) = 4u^2$$

and in consequence the equation

$$16t^2(25+6t^2+t^4)^2 - 32t^2(5+t^2)^4x + (5+t^2)^6x^2 = 0$$

would have a solution $x \in K$. The discriminant of the above quadratic polynomial is equal to

$$-64t^2(5+t^2)^6(625-100t^2-74t^4-4t^6+t^8)$$

and it is not a square in K, hence we get a contradiction. Similarly one can show that $T_1+(0,0) = ((u^2-1)^2, 0)$ is not in $2E_3(K)$. Finally, it is easy to check that $2T_2 = (0,0)$. The claim follows from that. $\square$

Lemma 6.2. *The group $E_3(\overline{\mathbb{Q}}(t))/E_3(\overline{\mathbb{Q}}(t))_{tors}$ is free abelian of rank 3. It is generated by the following points*

$$\begin{aligned}
P_1 &= (2(1+\sqrt{2})(-1+u)^2u, 2\sqrt{-1}(1+\sqrt{2})(-1+(\sqrt{2}-u)^2)(-1+u)^2u),\\
P_2 &= (2(u-1)^2, 2(-1+u)^2(-1+2u+u^2)),\\
P_3 &= (1-u^2, \frac{(-5+t^2)u(-1+u^2)}{5+t^2}),
\end{aligned}$$

where $u = \frac{2t}{5+t^2}$.

Proof. We follow the argument in the proof of [19, Proposition 4.2]. We put $K = \overline{\mathbb{Q}}(t)$. Let $(E_3(K)/E_3(K)_{tors}, \langle\cdot,\cdot\rangle_{E_3})$ denote the Mordell-Weil lattice with the height pairing $\langle\cdot,\cdot\rangle_{E_3}$. From the type of singular fibers, i.e. I_2 and I_4, cf. Table 3, we know that for each $P, Q \in E_3(K)/E_3(K)_{tors}$ we have $\langle P, Q\rangle_{E_3} \in \frac{1}{4}\mathbb{Z}$.

Consider the lattice $\Lambda = E_3(K)/E_3(K)_{tors}$ with the pairing $\langle\cdot,\cdot\rangle = 4\langle\cdot,\cdot\rangle_{E_3}$. Let Λ' be generated by P_1, P_2 and P_3. It is a sublattice of Λ of a finite index $n = [\Lambda : \Lambda']$. In the lattice Λ we have $\langle P_i, P_i\rangle = 4i$ for $i = 1,2,3$ and $\langle P_i, P_j\rangle = 0$ for $i \neq j$. Hence, the following equality holds for discriminants of lattices Λ and Λ' with the pairing $\langle\cdot,\cdot\rangle$

$$6 \cdot 4^3 = \Delta(\Lambda') = n^2\Delta(\Lambda).$$

Therefore, n divides 8. We want to show that $n = 1$. Consider the 2-descent homomorphism

$$\psi : E_3(K)/2E_3(K) \hookrightarrow K^*/(K^*)^2 \times K^*/(K^*)^2.$$

The pairing ψ is defined for points (x, y) in $E_3(K) \setminus E_3(K)[2]$ by the formula

$$\psi(x, y) = (x - e_1, x - e_2),$$

where $e_1 = 0$ and $e_2 = 4u^2$.

Let H denote the group generated by points P_1, P_2, P_3, T_1, T_2 and let G denote $E_3(K)$. The index n equals $[G : H]$. There exist elements $R_1, R_2, R_3 \in G$ such that G is generated by R_1, R_2, R_3, T_1, T_2 and H is generated by $aR_1, bR_2, cR_3, T_1, T_2$, where $n = abc$ and $a|b|c$. For $n = 8$, it follows that $(a, b, c) \in \{(1,1,8), (1,2,4), (2,2,2)\}$. For $n = 4$, we have $(a, b, c) \in \{(1,1,4), (1,2,2)\}$ and for $n = 2$ there is only one tuple $(a, b, c) = (1,1,2)$. Consider the modulo 2 map $\phi : G \to G/2G$ and $\eta = \psi \circ \phi$. The image $\eta(G)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$. If $n = 8$, then $\eta(H) \cong (\mathbb{Z}/2\mathbb{Z})^i$, where $1 \le i \le 3$. If $n = 4$, then $\eta(H) \cong (\mathbb{Z}/2\mathbb{Z})^i$, where $2 \le i \le 3$. If $n = 2$, then $\eta(H) \cong (\mathbb{Z}/2\mathbb{Z})^3$. Hence, to show that $H = G$ it is sufficient to prove that $\eta(H) \cong (\mathbb{Z}/2\mathbb{Z})^4$. We easily compute

$$\begin{aligned}
\eta(P_1) &= \left((t(t^2+5), (t^2+5)t\left(-5+\left(-2+2\sqrt{2}\right)t-t^2\right)\left(-5+\left(2+2\sqrt{2}\right)t-t^2\right)\right),\\
\eta(P_2) &= (1, t^4-4t^3+6t^2-20t+25),\\
\eta(P_3) &= (\left(t^2-2t+5\right)\left(t^2+2t+5\right), 1),\\
\eta(T_2) &= (t\left(t^2-2t+5\right)\left(t^2+2t+5\right)(t^2+5), t\left(t^4+4t^3+6t^2+20t+25\right)(t^2+5))
\end{aligned}$$

and prove that $|\eta(H)| = 16$, which proves the theorem. $\square$

Corollary 6.3. *The group $E_3(\mathbb{Q}(t))$ is isomorphic to $\mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The free part is generated by P_2, P_3. The torsion part is generated by T_1, $2T_2 = (0,0)$.*

Proof. First we prove that the rank of the group $E_3(\mathbb{Q}(t))$ equals 2. From Corollary 5.5 we know that $rank\, E_3(\mathbb{Q}(t)) \leq 3$. Since the points P_2 and P_3 are linearly independent it is enough to show that $rank\, E_3(\mathbb{Q}(t))$ is smaller than 3.

Suppose to the contrary that the rank of $H = E_3(\mathbb{Q}(t))$ equals 3. Then H is a finite index subgroup of the group $G = E_3(\overline{\mathbb{Q}}(t))$ generated by P_1, P_2, P_3, T_1 and T_2. Consider the 3-dimensional $\mathbb{Q}$-vector space $G_{\mathbb{Q}} = G \otimes_{\mathbb{Z}} \mathbb{Q}$. There is a natural Galois representation

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut(G_{\mathbb{Q}}).$$

For $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ and $P \in G$ we define $\sigma(P \otimes 1) = \sigma(P) \otimes 1$, where $\sigma(P)$ denotes the element in G such that σ acts on the coefficients of rational functions in the coordinates of P. If $\sigma(\sqrt{-1}) = -\sqrt{-1}$ and $\sigma(\sqrt{2}) = \sqrt{2}$, then $\sigma(P_1 \otimes 1) = -(P_1 \otimes 1)$. In the basis $\{P_1 \otimes 1, P_2 \otimes 1, P_3 \otimes 1\}$ of $G_{\mathbb{Q}}$, the matrix of the automorphism $\rho(\sigma)$ is

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence, the representation ρ is nontrivial. However, $G_{\mathbb{Q}} = H_{\mathbb{Q}}$, since we assumed that H is of finite index in G. The representation ρ acts trivially on $H_{\mathbb{Q}}$, which leads to a contradiction. Hence, H is not of finite index in G, which implies that $rank\, H = 2$.

If the Mordell-Weil lattice $E_3(\mathbb{Q}(t))/E_3(\mathbb{Q}(t))_{tors}$ were not generated by P_2 and P_3, then the lattice generated by those points would be of finite index greater than 1 in the full Mordell-Weil lattice. Then the lattice generated by P_1, P_2 and P_3 would be of index greater than 1 in the full Mordell-Weil lattice $E_3(\overline{\mathbb{Q}}(t))/E_3(\overline{\mathbb{Q}}(t))_{tors}$, which contradicts Lemma 6.2.

To conclude the proof, we compute the torsion part. Lemma 6.1 shows that the torsion defined over $\mathbb{Q}(t)$ is generated by $T_1 = (4u^2, 0)$ and $(0,0) = 2T_2$. It is the full torsion subgroup of $E_3(\mathbb{Q}(t))$. □

Proof of Theorem 1.3. From Corollary 5.5 it follows that $rank\, E_3(\overline{\mathbb{Q}}(t)) = 3$. Lemma 6.2 and Lemma 6.1 give explicit generators over $\overline{\mathbb{Q}}(t)$. Finally, Corollary 6.3 shows that the rank over $\mathbb{Q}(t)$ is 2 and it gives explicit generators. □

Proof of Theorem 1.1. We apply the specialization theorem (cf. [17, Theorem 11.4]) to the family

$$y^2 = x(x - (u^2 - 1)^2)(x - 4u^2) \tag{6.1}$$

with a rational parameter t and $u = \frac{2t}{5+t^2}$. The curve is nonsingular for any $t \neq 0$. Let $\frac{p}{q} = t$ denote a rational number where p and $q \neq 0$ are relatively prime integers. The maps $(a, b, c) \mapsto \frac{b}{c-a}$ and $\frac{P}{Q} \mapsto (P^2 - Q^2, 2PQ, P^2 + Q^2)$ are inverses of each other. Let $\frac{P}{Q} = u = \frac{2pq}{p^2+5q^2}$ where P and Q are relatively prime. Put $k = GCD(2pq, p^2 + 5q^2)$. Observe that P is even, while Q is odd, since 2-valuation of $2pq$ is always greater than the 2-valuation of $p^2 + 5q^2$. Therefore $P^2 + Q^2$ is odd and it is relatively prime to $2PQ$. Similarly, $P^2 + Q^2$ is odd and relatively prime to $2PQ$. Hence, the triple $(a, b, c) = (P^2 - Q^2, 2PQ, P^2 + Q^2)$ defines a smooth Pythagorean triple and the associated elliptic curve

$$y^2 = x(x - a^2)(x - b^2)$$

has the following two points

$$Q_1 = \left(\frac{1}{2}(a + b - c)^2, \frac{1}{2}(a + b)(a + b - c)^2\right),$$

$$Q_2 = \left(\frac{1}{2}a(a - c), \frac{1}{2}ab\frac{1}{k^2}\left(p^4 - 25q^4\right)\right).$$

The points Q_1 and Q_2 are obtained from

$$P_2 = (2(u-1)^2, 2(-1+u)^2(-1+2u+u^2))$$

and

$$P_3 = \left(1-u^2, \frac{(-5+t^2)\,u\,(-1+u^2)}{5+t^2}\right)$$

by the map $(x,y) \mapsto \left(x\frac{(a-c)^2}{4}, y\frac{(c-a)^3}{8}\right)$. The specialization theorem shows that the points Q_1 and Q_2 are linearly independent for almost all values of p and q as above. ☐

Remark 6.4. Observe that the point

$$(c^2, abc) = -2\left(\frac{1}{2}(a+b-c)^2, \frac{1}{2}(a+b)(a+b-c)^2\right)$$

is on the curve

$$y^2 = x(x-a^2)(x-b^2).$$

The point $\left(\frac{1}{2}(a+b-c)^2, \frac{1}{2}(a+b)(a+b-c)^2\right)$ corresponds to the point

$$\left(2(t-1)^2, 2(t-1)^2(-1+2t+t^2)\right)$$

via the inverse of the map $(x,y) \mapsto \left(x\frac{(a-c)^2}{4}, y\frac{(c-a)^3}{8}\right)$. The point

$$\left(2(t-1)^2, 2(t-1)^2(-1+2t+t^2)\right)$$

is a generator of the free part of the Mordell-Weil group over $\mathbb{Q}(t)$ on the curve

$$y^2 = x(x-(t^2-1)^2)(x-4t^2).$$

We prove this fact the next lemma.

Lemma 6.5. *The group $E_2(\overline{\mathbb{Q}}(t))$ is isomorphic to $\mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. The free part is generated by points.*

$$\begin{aligned} P_1 &= (2(1+\sqrt{2})(-1+t)^2 t, 2\sqrt{-1}(1+\sqrt{2})(-1+(\sqrt{2}-t)^2)(-1+t)^2 t), \\ P_2 &= (2(t-1)^2, 2(-1+t)^2(-1+2t+t^2)). \end{aligned}$$

The torsion part is generated by

$$\begin{aligned} T_1 &= (-4t^2, 0) \\ T_2 &= (2(-t+t^3), 2\sqrt{-1}(t^2-1)t(-1-2t+t^2)). \end{aligned}$$

The group $E_2(\mathbb{Q}(t))$ is generated by P_2, T_1 and $2T_2 = (0,0)$.

Proof. The torsion subgroup is computed similarly as in the proof of Lemma 6.1. We put $K = \overline{\mathbb{Q}}(t)$. Let $(E_2(K)/E_2(K)_{tors}, \langle\cdot,\cdot\rangle_{E_2})$ be the Mordell-Weil lattice with the height pairing $\langle\cdot,\cdot\rangle_{E_2}$. We compute easily $\langle P_1, P_1\rangle_{E_2} = \frac{1}{2}$, $\langle P_2, P_2\rangle_{E_2} = 1$ and $\langle P_1, P_2\rangle_{E_2} = 0$. In general, for each $P, Q \in E_2(K)/E_2(K)_{tors}$ the value of the pairing $\langle P, Q\rangle_{E_2}$ lies in $\frac{1}{4}\mathbb{Z}$ which follows by the type of singular fibers (cf. Table 2).

Consider the lattice $\Lambda = (E_2(K)/E_2(K)_{tors}$ with the pairing $\langle\cdot,\cdot,\rangle = 4\langle\cdot,\cdot\rangle_{E_2}$. Let Λ' be generated by P_1 and P_2. It is a sublattice of Λ of a finite index which we call $n = [\Lambda : \Lambda']$. For the lattice Λ we have $\langle P_1, P_1\rangle = 2$, $\langle P_2, P_2\rangle = 4$ and $\langle P_1, P_2\rangle = 0$. Hence, the following equality holds for discriminants of lattices Λ and Λ' with respect to the pairing $\langle\cdot,\cdot\rangle$

$$8 = \Delta(\Lambda') = n^2 \Delta(\Lambda).$$

Hence, n divides 2. We want to show that $n = 1$. Suppose to the contrary that $n = 2$. There exists a point $R \in E_2(K)$ of infinite order, such that

$$2R = aP_1 + bP_2 + T$$

for some $a, b \in \{0, 1\}$ and $T \in E_2(K)_{\text{tors}}$. So

$$4\langle R, R\rangle = \langle 2R, 2R\rangle = 2a^2 + 4b^2 = 2(a^2 + 2b^2).$$

This implies $2 \mid (a^2 + 2b^2)$. For $a, b \in \{0, 1\}$ there are pairs $(a, b) = (0, 0)$ and $(a, b) = (0, 1)$. For $(a, b) = (0, 0)$ we obtain the equation

$$2R = T$$

for a K-rational torsion point T. This implies that R is of finite order, hence a contradiction. For the pair $(a, b) = (0, 1)$ we obtain the equation

$$2R = P_2 + T$$

with a K-rational torsion point T. We consider only the cases $T = O$, $T = T_1$, $T = T_2$ and $T = T_1 + T_2$, since one can add a point from $2E_2(K)_{\text{tors}}$ to both sides.

Consider the 2-descent homomorphism

$$\psi : E_2(K)/2E_2(K) \hookrightarrow K^*/(K^*)^2 \times K^*/(K^*)^2.$$

The pairing is defined for non-torsion points (x, y) in $E_2(K)$ by the formula $\psi(x, y) = (x - e_1, x - e_2)$ where $e_1 = 0$ and $e_2 = 4t^2$. We check using MAGMA that $\psi(P_2 + T) \neq (1, 1)$ for $T \in \{O, T_1, T_2, T_1 + T_2\}$. This proves that the assumption $n = 2$ leads to a contradiction. Hence $\Lambda = \Lambda'$, proving that the rank of $E_2(K)$ is two.

Now we prove that the group $E_2(\mathbb{Q}(t))$ is generated by P_2, T_1 and $2T_2$. For the torsion part, observe that $E_2(\mathbb{Q}(t))_{\text{tors}} \subset E_2(\overline{\mathbb{Q}}(t))_{\text{tors}}$. The group $E_2(\overline{\mathbb{Q}}(t))_{\text{tors}}$ is generated by T_1 and T_2. Since T_2 is not $\mathbb{Q}(t)$-rational, the group $E_2(\mathbb{Q}(t))_{\text{tors}}$ is generated by T_1 and $2T_2 = (0, 0)$. We know that the rank of $E_2(\overline{\mathbb{Q}}(t))$ is 2. Hence, the rank of $E_2(\mathbb{Q}(t))$ is at most 2. Assume it equals 2.

Then there exists a point R defined over $\mathbb{Q}(t)$ such that $R = aP_1 + bP_2 + T$ for some integers $a \neq 0$ and b and a torsion point T. Since $4T = O$, we have

$$4R = 4aP_1 + 4bP_2. \tag{6.2}$$

Recall that

$$P_1 = (2(1 + \sqrt{2})(-1 + t)^2 t, 2\sqrt{-1}(1 + \sqrt{2})(-1 + (\sqrt{2} - t)^2)(-1 + t)^2 t).$$

We choose an automorphism $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ which acts on the coefficients of rational functions in the coordinates of P_1 by the formula $\sigma(\sqrt{-1}) = -\sqrt{-1}$, $\sigma(\sqrt{2}) = \sqrt{2}$. The action of σ commutes with the addition morphism on the curve E_2 which is defined over $\mathbb{Q}(t)$. Applying σ to both sides of (6.2) we get $8cP_1 = O$, because $\sigma(P_1) = -P_1$ and $\sigma(P_2) = P_2$. This gives a contradiction since P_1 is a non-torsion point.

If the Mordell-Weil lattice $E_2(\mathbb{Q}(t))/E_2(\mathbb{Q}(t))_{tors}$ were not generated by P_2, then the lattice generated by this point would be of finite index greater than 1 in the full Mordell-Weil lattice. Then the lattice generated by P_1 and P_2 would be of index greater than 1 in the full Mordell-Weil lattice $E_2(\overline{\mathbb{Q}}(t))/E_2(\overline{\mathbb{Q}}(t))_{tors}$, which contradicts what has been proven already. □

Proof of Theorem 1.2. This follows from Lemma 6.5 where we observed that the curves

$$y^2 = x(x-1)(x - \left(\frac{2t}{t^2-1}\right)^2),$$
$$y^2 = x(x - (t^2-1)^2)(x - 4t^2)$$

were isomorphic over $\mathbb{Q}(t)$. □

Remark 6.6. It is natural to ask what is the rank of the Mordell-Weil group of a curve

$$y^2 = x(x - \alpha a^2)(x - \beta b^2),$$

where $\alpha a^2 + \beta b^2 + \gamma c^2 = 0$ for some $\alpha, \beta, \gamma \in \mathbb{Z}$. In particular, one would like to know what is the upper bound of the rank in such a big family. We hope to return to this question in the future.

Acknowledgments

The author would like to thank Wojciech Gajda for suggesting this research problem and for many helpful remarks. He thanks Adrian Langer for many helpful comments. The author gratefully acknowledges the many helpful suggestions of Remke Kloosterman, especially drawing the author's attention to the method of twisting and the application of the Artin-Tate conjectures.

References

[1] M. Artin and H. P. F. Swinnerton-Dyer, *The Shafarevich-Tate conjecture for pencils of elliptic curves on $K3$ surfaces*, Invent. Math. **20** (1973), 249–266.
[2] Wolf P. Barth, Klaus Hulek, Chris A. M. Peters, and Antonius Van de Ven, *Compact complex surfaces*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 4, Springer-Verlag, Berlin, 2004.
[3] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language.*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).
[4] François R. Cossec and Igor V. Dolgachev, *Enriques surfaces. I*, Progress in Mathematics, vol. 76, Birkhäuser Boston Inc., Boston, MA, 1989.
[5] Andreas-Stephan Elsenhans and Jörg Jahnel, *The picard group of a k3 surface and its reduction modulo p*, Algebra Number Theory **5** (2011), no. 8, 1027–Ũ1040.
[6] F. A. Izadi, K. Nabardi, and F. Khoshnam, *On a Family Of Elliptic Curves With Positive Rank arising from Pythagorean Triples*, ArXiv e-prints (2010), arXiv:1012.5837v4.
[7] S. L. Kleiman, *Algebraic cycles and the Weil conjectures*, Dix esposés sur la cohomologie des schémas, North-Holland, Amsterdam, 1968, pp. 359–386.
[8] Remke Kloosterman, *Elliptic $K3$ surfaces with geometric Mordell-Weil rank 15*, Canad. Math. Bull. **50** (2007), no. 2, 215–226.
[9] James S. Milne, *On a conjecture of Artin and Tate*, Ann. of Math. (2) **102** (1975), no. 3, 517–533.
[10] ———, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.
[11] ———, *Values of zeta functions of varieties over finite fields*, Amer. J. Math. **108** (1986), no. 2, 297–360.
[12] David Mumford, *Selected papers on the classification of varieties and moduli spaces*, Springer-Verlag, New York, 2004, With commentaries by David Gieseker, George Kempf, Herbert Lange and Eckart Viehweg.
[13] Matthias Schütt, *$K3$ surfaces with Picard rank 20*, Algebra Number Theory **4** (2010), no. 3, 335–356.
[14] T. Shioda and M. Schütt, *Elliptic surfaces*, ArXiv e-prints (2010), arXiv:0907.0298v3.
[15] Tetsuji Shioda, *On the Mordell-Weil lattices*, Comment. Math. Univ. St. Paul. **39** (1990), no. 2, 211–240.
[16] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
[17] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
[18] Jaap Top and Frank De Zeeuw, *Explicit elliptic $K3$ surfaces with rank 15*, Rocky Mountain J. Math. **39** (2009), no. 5, 1689–1697.
[19] Ronald van Luijk, *A $K3$ surface associated with certain integral matrices having integral eigenvalues*, Canad. Math. Bull. **49** (2006), no. 4, 560–577.
[20] ———, *An elliptic $K3$ surface associated to Heron triangles*, J. Number Theory **123** (2007), no. 1, 92–119.